The iPhone 5s: How Secure is the Touch ID?

By Sharon D. Nelson, Esq. and John W. Simek

It came as no surprise that the new iPhone was hacked within a couple days of its release. The hack was hyped in the headlines all out of proportion to the hack itself. And the security vulnerability uncovered was really old and tattered. We have known for a long time that fingerprints could be compromised.

But it was downright fun to read in SC Magazine that there was already a crowdsourced bounty to crack the iPhone 5s – the first Apple product to feature authentication via a fingerprint scan – even before the phone was released. The bounty was around $20,000 when we saw it, though the amount dropped later when someone reneged on their pledge.

Within two days of the phone's release, the German biometrics hacking team of the Chaos Computer Club (CCC) - an interesting name - successfully bypassed the biometric security of Apple's TouchID.

Here is the methodology that was used as described by the CCC. "First, the residual fingerprint from the phone is either photographed or scanned with a flatbed scanner at 2400 dpi. Then the image is converted to black & white, inverted and mirrored. This image is then printed onto a transparent sheet at 1200 dpi. To create the mold, the mask is then used to expose the fingerprint structure on photo-sensitive PCB material. The PCB material is then developed, etched and cleaned. After this process, the mold is ready. A thin coat of graphite spray is applied to ensure an improved capacitive response. This also makes it easier to remove the fake fingerprint. Finally a thin film of white wood glue is smeared into the mold. After the glue cures the new fake fingerprint is ready for use."

We have to say this this methodology doesn't sound all that easy to us. But it would certainly be relatively simple for someone who was targeting a specific phone and knew what they were doing. We do agree with CCC's statement that "It is plain stupid to use something that you can´t change and that you leave

everywhere every day as a security token." And we agree that whereas a law enforcement officer can't compel you to divulge your PIN, they could swipe your phone over your handcuffed hands.

There are some security safeguards in place. You can't unlock the phone with a fingerprint only if the device hasn't been unlocked in 48 hours or has been reset – then you need the traditional PIN.

Apple has emphasized that the fingerprint data will be encrypted and stored locally on a device – never uploaded to a cloud. But still . . . we take our fingerprints everywhere we go – is this really a good security mechanism?

It would have been a true advancement if Apple had permitted users to choose BOTH fingerprint authentication and a PIN. But this option is not available, even to those who would elect two-factor authentication in the name of security. Still, we are mindful that the Touch ID is better than no PIN – which is where many iPhone users are now. It may even be more secure than a four digit PIN as well. And to put things in context, any evildoer must steal your phone as well as your fingerprint to get to your data. The odds of that happening are not great – unless you are targeted.

Our recommendation remains the complex password, certainly for lawyers who do carry sensitive data on their phones. Also remember that the iPhone even stores data (e.g. screen shots) that you didn't intentionally save, which may include confidential information.

On a side note, the worst Apple flaw we've seen is the issuance of iOS 7, which included an easy way to deactivate 'Find my iPhone' or 'Find My iPad' even when the device is locked. All a bad guy has to turn do is turn on airplane mode which can be done via Siri or in the Control Center, a feature new to iOS. Since that will disable mobile and Wi-Fi features, the location apps are defeated. How the Apple security geniuses let that one get through is beyond us. If you are like most security specialists and tired of Apple's slow response, just go to the Control Center and turn off the "Access on Lock Screen" feature. (Last minue update: Apple released iOS 7.0.2, a minor patch, on September 26th, and it fixes two lock

screen bugs, but it is unclear as we go to press whether the bugs identified above are resolved).

It is gratifying to see Apple paying more attention to security, even if there are some missteps along the way. Security for smartphones will continue to evolve. The technological futurists all recognize that we live in a "Passwords are Dying" world and that two-factor authentication is a certain requirement for lawyers in the fairly near term. We are fans of tokens (something you have) along with passwords (something you know) as the mechanism for authenticating. The problem with biometrics – fingerprints, retina scans, etc. – is that they can all ultimately be compromised.

And this is why all lawyers should attend a security CLE update at least once a year – nothing evolves as fast as technology and the recommended means of securing it!

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com.